IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
NORTHERN DIVISION

UNITED STATES OF AMERICA	**:**	
	:	
v.	**:**	**Criminal No.: WDQ-14-0116**
	:	
MASTER GIDDINS	**:**	

oo0oo

GOVERNMENT'S RESPONSE TO MOTION TO SUPPRESS CELL SITE LOCATION DATA

Now comes the United States of America by its attorneys, Rod J. Rosenstein, United States Attorney, and A. David Copperthite, Assistant United States Attorney for said District, hereby responding as follows to the pre-trial motion to suppress cell site location data and its fruits (derivative evidence) filed by the Defendant in the above captioned case.

INTRODUCTION

The Defendant is charged with three counts of bank robbery in violation of 18 U.S.C. §2113 and conspiracy to commit bank robbery in violation of 18 U.S.C. §371. Defendant has filed a motion to suppress cell site location data and its fruits (derivative evidence). The government files this response and respectfully requests this Court deny the motion.

Facts

On September 25, 2013, Defendant entered the M&T Bank at 329 W. Baltimore Street in Baltimore City. Defendant was wearing women's clothing and a long black wig. Defendant handed a note to the teller stating that he had a bomb and Defendant demanded money be placed into a black and white polka dot cosmetic bag he handed to the teller. The teller placed cash and a

GPS tracking device into the cosmetic bag and handed it back to Defendant. Defendant fled the bank but discarded the GPS tracking device out the car window. Police recovered the GPS tracking device in the bus lane on Baltimore Street. It had been run over by a vehicle but agents were able to recover some wig fibers from the tracking device. Czekiah Fludd, an unindicted co-defendant was the getaway driver, and drove Defendant's Ford Focus automobile from the scene.

On September 26, 2013, Defendant provided the automobile to Czekiah Fludd and another female, Ashley Fitz, so they could rob a second bank. Fitz and Fludd drove the Ford Focus to the 1st Mariner Bank at 4800 Painters Mill Road in Owings Mills, Maryland. Before entering the bank, Fludd drove the Ford Focus to an Exxon station near the bank and Fludd went into the station and obtained blank Maryland lottery tickets. Fludd and or Fitz then wrote a similar note on a blank lottery ticket to hand to the teller at 1st Mariner Bank. Fitz went into the bank wearing the same long black wig and using the same black and white polka dot cosmetic bag which she handed to the teller with the note. Fitz was given an amount of cash by the teller and ran from the bank. A nearby construction worker saw Fitz and Fludd get into the silver Ford Focus belonging to Giddins. They were also captured on video at the Exxon station where Fludd obtained the blank lottery tickets to write the note. The proceeds of the robbery were split between Fludd, Fitz and Giddins.

The following day, September 27, 2013, Giddins again provided his Ford Focus automobile to Fitz and Fludd who were joined by a third female co-conspirator named Alexis Chandler. Fludd drove Fitz and Chandler to Baltimore County Savings Bank at 515 Eastern Avenue in Baltimore County. Fitz and Chandler, wearing wigs, entered the Bank and again produced notes stating they had a bomb and demanded money. The tellers provided them with

cash and Fitz was given a dye pack as well. After leaving the bank, they got into the Ford Focus driven by Fludd. The dye pack exploded and Fitz tossed the handbag with the exploded dye pack out of the window. The unindicted co-defendants also discarded the wigs and some other items. Police stopped the car after receiving a broadcast of the description of the suspects and the silver Ford Focus vehicle. Evidence was recovered from the car and the scene. Fitz and Chandler provided statements to investigators after being advised of their rights. Fitz and Chandler admitted to the robberies and their involvement. All three banks were FDIC insured.

Defendant responded to Baltimore County police headquarters to obtain the return of his vehicle. Defendant was placed in an interrogation room. Initially Defendant was advised that he was free to go. He answered questions voluntarily, which were the equivalent of normal "booking questions", such as his name, address, employment, phone number, date of birth and social security number. Defendant was advised of his rights. Defendant continued to answer questions and after asking why he was being questioned, police advised him of his suspected involvement in the robberies. He asked for a lawyer later in the questioning so questioning ceased.

Defendant voluntarily supplied the phone number to his cellular telephone. In furtherance of their investigation, agents sought and obtained through undersigned counsel, a court order pursuant to 18 U.S.C. §2703(d) for subscriber information, historical call records, and historical GPS/cell site information. On December 20, 2013, United States Magistrate Judge Susan K. Gauvey found that the government had "provided specific, articulable facts and there are reasonable grounds to believe the subscriber information, historical call records and GPS/cell site information are relevant and material to the ongoing investigation of possible violations of 18

U.S.C. §2113." **Exhibit 1.** The data obtained indicated Defendant's sprint cellular phone communicated with two cell towers located near the M&T bank on September 25, 2013 at the time of the robbery.

Argument

I. A Cell Phone Customer Has No Privacy Interest in Historical Cell-Site Records Because They Are Business Records Created and Held by a Cell Phone Provider.

The historical cell-site records at issue in this case consist of business records created and maintained by Sprint for its own purposes. The records contain a list of incoming and outgoing phone calls, the time and duration of each call, and the cellular tower used by the phone both at the beginning and at the termination of the call. The records do not reflect the content of any conversation or the specific location of the phone itself.

A cell phone customer has no Fourth Amendment privacy interest in historical cell-site records because such records are business records held by a third party, and are not the customer's private papers. In *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court rejected a Fourth Amendment challenge to a third-party subpoena for bank records and explained that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." *Miller*, 425 U.S. at 440. As the Court observed, the records "pertain[ed] to transactions to which the bank was itself a party." *Id.* at 441. In rejecting the challenge to the subpoena, the Court held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used

only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443. *Miller*'s reasoning squarely applies to historical cell-site records. First, cell-site records are not a customer's private papers. Once a customer places a call, he or she thereafter has no control over cell-site records relating to his or her phone. Moreover, although a customer is likely to be aware that the cell phone company will assign a cell tower to handle her call, the customer typically does not know which cell tower is assigned to process it. Second, cell-site records are business records of the provider. The choice to create and store historical cell-site records is made by the provider, and the provider controls the format, content, and duration of the records it chooses to create and retain. In addition, individual customers do not generally have access to those records, and could not be expected to produce them in response to a subpoena. Third, cell-site records pertain to transactions to which the cell phone company was a party. The assignment of a particular cell tower to process a call is made by the cell phone company to facilitate the functioning of its network. Thus, under *Miller*, a customer's historical cell-site records are not protected by the Fourth Amendment because they are the phone company's business records rather than a customer's private papers.

The Supreme Court's reasoning in *Smith v. Maryland*, 442 U.S. 735 (1979), further demonstrates that a customer has no reasonable expectation of privacy in cell-site information. In *Smith*, the telephone company installed a pen register at the request of the police to record numbers dialed from the defendant's telephone. The Supreme Court held both that telephone users have no subjective expectation of privacy in dialed telephone numbers and that any such expectation is not

one that society is prepared to recognize as reasonable. *See Smith*, 442 U.S. at 742-44. The Court's reasoning in *Smith* applies equally to cell-site records.

Indeed, in *Smith*, the Court stated: "[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. Similarly, cell phone users understand that they must send a signal that is received by a cell phone company's antenna if the company is going to route their call to its intended recipient.

In *Smith*, the Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, "this expectation is not one that society is prepared to recognize as reasonable." 442 U.S. at 743 (internal quotation marks omitted). The Court explained that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and held that the user "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 743-44. Here, a cell phone user voluntarily transmits a signal to a cell tower for his call to be connected, and the provider thereby creates records, for its own business purposes, regarding which of its cell towers it used to complete the call. If anything, the privacy interest in cell-site information is even less than the privacy interest in a dialed phone number: the location of the cell phone tower handling a customer's call is generated internally by the phone company and is not typically known by the customer. For all of these reasons, a customer's Fourth Amendment rights are not violated when

the phone company reveals to the government its own internal records that were never in the possession or control of the customer.

Courts have applied the principle that information revealed to a third party may be disclosed to the government in a wide variety of other contexts. The Supreme Court has applied this third-party principle to confidential statements made in the presence of an informant, *see Hoffa v. United States*, 385 U.S. 293, 302 (1966), as well as to financial and other records in the hands of third-party businesses. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *see also Donaldson v. United States*, 400 U.S. 517, 522-23 (1971) (holding that taxpayer was not entitled to intervene in proceeding to enforce summons for his employment records and stating, "what is sought here by the Internal Revenue Service . . . is the production of Acme's records and not the records of the taxpayer"). Moreover, the Fourth Circuit recently applied the same principles to cell phone records in *United States v. Clenney*, 631 F.3d 658, 666 (4th Cir. 2011), and to internet subscriber information from Yahoo! Inc., in *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010). Notably, other appellate courts have applied this third-party principle to records of communications ranging from telephone billing records to ISP subscriber information to IP addresses of websites visited. *See Reporters Committee for Freedom of Press v. AT&T*, 593 F.2d 1030, 1043 (D.C. Cir. 1978) (rejecting Fourth Amendment challenge to subpoena for telephone records and explaining that when an individual transacts business with others, "he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair."); *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an

internet provider is not protected by the Fourth Amendment's privacy expectation."); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that e-mail users have no reasonable expectation of privacy in the to/from addresses of their messages or in the IP addresses of websites visited).

Numerous courts have relied on *Smith* and *Miller* and rejected Fourth Amendment challenges to the acquisition of historical cell-site records via § 2703(d) orders. Indeed, the Fifth Circuit recently became the first court of appeals to address whether a warrant is required to compel the disclosure of historical cell-site records; it held that a § 2703(d) order is sufficient. *See In re Application*, 724 F.3d 600, 615 (5th Cir. 2013) (hereinafter, "*Fifth Circuit Decision*"). The court explained that when the government uses a § 2703(d) order to obtain cell-site records, it "merely comes in after the fact and asks a provider to turn over records the provider has already created." *Id.* at 612. Thus, the court concluded that "[c]ell site data are business records and should be analyzed under that line of Supreme Court precedent." *Id*. at 615.

In addition, many district courts have relied on *Smith* and *Miller* to uphold the use of § 2703(d) orders to obtain historical cell-site records. *See, e.g.*, *United States v. Wilson*, 2013 WL 1129199, at *6-*7 (N.D. Ga. Feb. 20, 2013) (denying motion to suppress historical cell-site data); *United States v. Madison*, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012) (same); *United States v. Dye*, 2011 WL 1595255, at *9 (N.D. Ohio April 27, 2011) (same); *United States v. Velasquez*, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (same); *United States v. Benford*, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010); *United States v. Suarez-Blanca*, 2008 WL 4200156, at *8-*11 (N.D. Ga. April 21, 2008) (same). *But see In re Application of United States*, 620 F.3d 304,

313, 317 (3d Cir. 2010) (asserting that location information is not voluntarily conveyed to a cell phone provider, but nevertheless stating that historical cell-site records are "obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination") (hereinafter "*Third Circuit Decision*"); *In re Application of United States*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (holding that a warrant is required to compel disclosure of historical cell-site records).

II. The Government Obtained the Defendant's Phone's Cell-Site Records in Good Faith Reliance on a Federal Statute, Case Law, and an Order Issued by a Magistrate Judge.

Assuming arguendo that a Fourth Amendment violation occurred in securing historical cell-site data associated with the phone used by the defendant, suppression would not be the appropriate remedy. "The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009).

First, suppression is not an appropriate remedy because the government obtained the historical cell-site records in objectively reasonable reliance on the Stored Communications Act. In *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987), the Supreme Court held that an officer's objectively reasonable reliance on a statute – even where a court concludes in hindsight that the statute is constitutionally infirm – bars application of the exclusionary rule. "Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature." *Id.* The Court reasoned that "penalizing the officer for the [legislature's] error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id.* at 350. Under

Krull, reliance on a duly enacted statute is unreasonable "if, in passing the statute, the legislature wholly abandoned its responsibility to enact constitutional laws." *Id.* at 355.

Here, the government's reliance on the Stored Communications Act to obtain the defendant's historical cell-site records was objectively reasonable. As a statutory matter, a § 2703(d) order may be used to compel disclosure of cell-site records because the records fall within the scope of 18 U.S.C. § 2703(c)(1). In particular, § 2703(c)(1)(B) requires a provider "to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)" pursuant to a § 2703(d) order. *See Third Circuit Decision*, 620 F.3d at 313 (holding that cell-site records are "obtainable under a § 2703(d) order").

Moreover, it was objectively reasonable for the government to use a § 2703(d) order to obtain the defendant's historical cell-site records because using a § 2703(d) order was not "clearly unconstitutional." To begin, there is "a strong presumption of constitutionality" with respect to federal statutes that are challenged on Fourth Amendment grounds. *United States v. Watson*, 423 U.S. 411, 416 (1976). Furthermore, as discussed above, using a § 2703(d) order to compel disclosure of cell-site records is supported both by Supreme Court precedent (including *Miller* and *Smith v. Maryland*) and Fourth Circuit precedent (including *Bynum* and *Clenney*). *See supra.* Therefore, under *Davis v. United States*, 131 S.Ct. 2419 (2011), the exclusionary rule does not apply. *Id*. at 2429 ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule.").

In addition, at the time the § 2703(d) orders at issue in this case were issued in 2013, the strong weight of the non-binding decisions of courts in other circuits supported using § 2703(d)

orders to obtain historical cell-site records. *See supra.* (citing *Dye*, *Velasquez*, *Benford*, and *Suarez-Blanca*). Thus, because using a § 2703(d) order to obtain historical cell-site records was not clearly unconstitutional at the time that the government secured the instant data, the exclusionary rule does not apply in this case. *See also United States v. McCullough*, 2013 WL 1729712, at *1 (2d Cir. Apr. 23, 2013) (unpub.) (holding that defendant was not prejudiced by counsel's failure to move to suppress cell-site information because the defendant could not show that § 2703 was "clearly unconstitutional" under *Krull*); *United States v. Jones*, 908 F. Supp. 2d 203, 214-16 (D.D.C. 2012) (rejecting motion to suppress cell-site records based on good faith reliance on § 2703).

That the § 2703(d) order was issued by a neutral magistrate judge further demonstrates that the government's reliance on them was not unreasonable. *See United States v. Leon*, 468 U.S. 897, 921 (1984) ("In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient."); *Suarez-Blanca*, 2008 WL 4200156 at *12-*13 (applying *Leon* to § 2703(d) order for cell-site records). Here, the Magistrate Judge applied the correct standard under the Stored Communications Act and found that law enforcement offered specific and articulable facts in support of the application. **Exh. 1.** The government is nevertheless entitled to rely on the judgment of the magistrate judge except in unusual circumstances, such as where the magistrate has "wholly abandoned his judicial role." *Leon*, 468 U.S. at 923. Thus, because the § 2703(d) orders to Sprint were issued by a neutral magistrate judge and was authorized by the Stored Communications Act, as interpreted by numerous courts, suppression is not an available remedy in this case.

Conclusion

For the foregoing reasons, the government respectfully requests the motion to suppress historical cell site date and derivative evidence be denied.

Respectfully submitted,

ROD J. ROSENSTEIN
UNITED STATES ATTORNEY

By: /s/
A. David Copperthite
Assistant United States Attorney

Certificate of Service

The foregoing Response to Motion to Suppress Cell Site Location Data and Its Fruits was electronically filed to Gary Christopher, First Assistant Federal Defender on this ____ day of August, 2014.

/s/
A. David Copperthite
Assistant United States Attorney